SCC P1544 WO 00
PCT/JP00/09023

JP00/09023 20.12.00

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年１２月２１日

出願番号
Application Number: 平成１１年特許願第３６３４６５号

出願人
Applicant (s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２０００年 ９月１８日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３０７５４７９

【書類名】　特許願

【整理番号】　9900962207

【提出日】　平成11年12月21日

【あて先】　特許庁長官　近藤　隆彦　殿

【国際特許分類】　G06F　1/00

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　佐古　曜一郎

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　所　眞理雄

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　猪口　達也

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　木島　薫

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100082762

【弁理士】

【氏名又は名称】　杉浦　正知

【電話番号】　03-3980-0339

【手数料の表示】

【予納台帳番号】　043812

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9708843

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子マネー、電子利用権、課金システムおよび情報処理装置

【特許請求の範囲】

【請求項１】　現金に相当する効力を有する電子マネーであって、

そのセキュリティを発行元または管理者が変更可能とされたことを特徴とする電子マネー。

【請求項２】　コンテンツの再生等のソフトウェアの利用を可能とする電子利用権であって、

そのセキュリティを発行元または管理者が変更可能とされたことを特徴とする電子利用権。

【請求項３】　請求項１または２において、

上記セキュリティが暗号化の鍵、上記鍵の鍵長、エラー検出および／または訂正コード、または有効期間であることを特徴とする電子マネーまたは電子利用権。

【請求項４】　請求項１または２において、

上記変更が所定期間毎になされることを特徴とする電子マネーまたは電子利用権。

【請求項５】　請求項１または２において、

上記変更が上記発行元または管理者の必要に応じてなされることを特徴とする電子マネーまたは電子利用権。

【請求項６】　請求項１または２において、

上記変更がなされた後、一定期間経過後に上記変更前のものを無効とすることを特徴とする電子マネーまたは電子利用権。

【請求項７】　請求項２において、

上記ソフトウェアは、オーディオデータ、ビデオデータ、静止画像データ、文字データ、コンピュータグラフィックデータ、ゲームソフトウェア、およびコンピュータプログラムの内の少なくとも１つであることを特徴とする電子利用権。

【請求項８】　圧縮符号化および／または暗号化されたソフトウェアが配付され、配付されたソフトウェアをユーザが復号するに際し、ユーザが所有する電

子マネーを介して課金処理がなされるようにした課金システムであって、

電子マネーのセキュリティを発行元または管理者が変更可能とされたことを特徴とする課金システム。

【請求項９】　圧縮符号化および／または暗号化されたソフトウェアが配付され、配付されたソフトウェアをユーザが復号するに際し、ユーザが所有する電子利用権を介して課金処理がなされるようにした課金システムであって、

電子利用権のセキュリティを発行元または管理者が変更可能とされたことを特徴とする課金システム。

【請求項１０】　請求項８または９において、

上記セキュリティが暗号化の鍵、上記鍵の鍵長、エラー検出および／または訂正コード、または有効期間であることを特徴とする課金システム。

【請求項１１】　請求項８または９において、

上記変更が所定期間毎になされることを特徴とする課金システム。

【請求項１２】　請求項８または９において、

上記変更が上記発行元または管理者の必要に応じてなされることを特徴とする課金システム。

【請求項１３】　請求項８または９において、

上記変更がなされた後、一定期間経過後に上記変更前のものを無効とすることを特徴とする課金システム。

【請求項１４】　請求項８または９において、

ユーザが所有する電子マネーまたは電子利用権を上記発行元または管理者が買い取るか、または有効な電子マネーまたは電子利用権へ交換することを特徴とする課金システム。

【請求項１５】　請求項８または９において、

ユーザの復号の結果が電子マネーまたは電子利用権で許容された範囲に達したタイミングで、電子マネーまたは電子利用権の要求を発生することを特徴とする課金システム。

【請求項１６】　請求項８または９において、

上記ソフトウェアは、オーディオデータ、ビデオデータ、静止画像データ、文

字データ、コンピュータグラフィックデータ、ゲームソフトウェア、およびコンピュータプログラムの内の少なくとも１つであることを特徴とする課金システム。

【請求項１７】　電子マネーまたは電子利用権を用いることによって稼働しているシステムであって、

電子マネーまたは電子利用権のセキュリティチェックを行い、

セキュリティチェックの結果が正しくないときには、システムの稼働の停止、並びにセキュリティチェックの結果が正しくないことの通知の少なくとも一方を行うことを特徴とする課金システム。

【請求項１８】　圧縮符号化および／または暗号化されたソフトウェアが配付され、配付されたソフトウェアをユーザが復号するに際し、ユーザが所有する電子マネーまたは電子利用権を介して課金処理がなされるようにした課金システムであって、

電子マネーまたは電子利用権のセキュリティチェックを行い、

セキュリティチェックの結果が正しくないときには、システムの稼働の停止、並びにセキュリティチェックの結果が正しくないことの通知の少なくとも一方を行うことを特徴とする課金システム。

【請求項１９】　配付された圧縮符号化および／または暗号化されたソフトウェアを復号するに際し、電子マネーまたは電子利用権を介して課金処理がなされるようにした情報処理装置であって、

電子マネーまたは電子利用権のセキュリティチェックを行い、

セキュリティチェックの結果が正しくないときには、ソフトウェアの復号の停止、並びにセキュリティチェックの結果が正しくないことの通知の少なくとも一方を行うことを特徴とする情報処理装置。

【請求項２０】　請求項１７、１８または１９において、

上記セキュリティチェックが暗号化の復号の結果、エラー検出および／または訂正の結果、または有効期間のチェックであることを特徴とする情報処理装置。

【請求項２１】　請求項１７、１８または１９において、

上記セキュリティチェックは、復号がされた後に残りの電子マネーまたは電子

利用権が正しい状態かどうかをチェックすることでなされることを特徴とするシステムまたは装置。

【請求項２２】　請求項１７、１８または１９において、

上記通知が電子マネーまたは電子利用権の発行元または管理者に対してなされることを特徴とするシステムまたは装置。

【請求項２３】　請求項１７、１８または１９において、

上記通知がユーザに対してなされることを特徴とするシステムまたは装置。

【請求項２４】　請求項１７、１８または１９において、

上記通知がユーザに対してなされることを特徴とするシステムまたは装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、例えば音楽配信に適用される電子マネー、電子利用権、課金システムおよび情報処理装置に関する。

【０００２】

【従来の技術】

現金と同様に流通する電子マネーが実用化されようとしている。電子マネーは、ＩＣカードに蓄積する。電子マネーとしては、プリペイド型、後払い型がある。さらに、インターネットとパーソナルコンピュータ（パソコン）とを使用して、自分の金融機関の口座からＩＣカードに入金したり、未使用分を口座に入金することも提案されている。また、電話使用料、乗車券等の電子利用権をＩＣカード、特に、非接触型のＩＣカードを介して実現する試みもなされている。

【０００３】

これらの電子マネー、電子利用権は、情報をＩＣカードに蓄積するので、既存の磁気ストライプ型のカードに比して、偽造が難しい利点がある。また、セキュリティ対策として、リーダ・ライタとＩＣカードと間でやり取りされるデータが暗号化されることが考えられている。

【０００４】

【発明が解決しようとする課題】

しかしながら、たとえ暗号化を行っていても、電子マネー、電子利用権のセキュリティが充分であるとは言えない。また、電子マネー、電子利用権を配信された音楽等のディジタルコンテンツを利用するための対価として使用することが考えられる。ディジタルコンテンツ自身に対しては、強力な暗号化や、コピープロテクション等が施されているのと比較して、電子マネー、電子利用権のセキュリティが高くはなかった。また、ディジタルコンテンツの利用と、電子マネー、電子利用権との共同作業がないたとも、セキュリティの面で弱い原因となっていた。さらに、ディジタルコンテンツは、電子マネー、電子利用権とは異なり、一旦流通すると、一元管理が難しく、コンテンツに対する暗号が破られたような場合に、システムの変更に多大な労力を要する。

【０００５】

したがって、この発明の目的は、このような点に鑑み、よりセキュリティを向上することができる電子マネー、電子利用権、課金システムおよび情報処理装置を提供することにある。

【０００６】

【課題を解決するための手段】

上述した課題を解決するために、請求項１の発明は、現金に相当する効力を有する電子マネーであって、

そのセキュリティを発行元または管理者が変更可能とされたことを特徴とする電子マネーである。

【０００７】

請求項２の発明は、コンテンツの再生等のソフトウェアの利用を可能とする電子利用権であって、

そのセキュリティを発行元または管理者が変更可能とされたことを特徴とする電子利用権である。

【０００８】

請求項８の発明は、圧縮符号化および／または暗号化されたソフトウェアが配

付され、配付されたソフトウェアをユーザが復号するに際し、ユーザが所有する電子マネーを介して課金処理がなされるようにした課金システムであって、

電子マネーのセキュリティを発行元または管理者が変更可能とされたことを特徴とする課金システムである

【０００９】

請求項９の発明は、圧縮符号化および／または暗号化されたソフトウェアが配付され、配付されたソフトウェアをユーザが復号するに際し、ユーザが所有する電子利用権を介して課金処理がなされるようにした課金システムであって、

電子利用権のセキュリティを発行元または管理者が変更可能とされたことを特徴とする課金システムである。

【００１０】

請求項１７の発明は、電子マネーまたは電子利用権を用いることによって稼働しているシステムであって、

電子マネーまたは電子利用権のセキュリティチェックを行い、

セキュリティチェックの結果が正しくないときには、システムの稼働の停止、並びにセキュリティチェックの結果が正しくないことの通知の少なくとも一方を行うことを特徴とする課金システムである。

【００１１】

請求項１８の発明は、圧縮符号化および／または暗号化されたソフトウェアが配付され、配付されたソフトウェアをユーザが復号するに際し、ユーザが所有する電子マネーまたは電子利用権を介して課金処理がなされるようにした課金システムであって、

電子マネーまたは電子利用権のセキュリティチェックを行い、

セキュリティチェックの結果が正しくないときには、システムの稼働の停止、並びにセキュリティチェックの結果が正しくないことの通知の少なくとも一方を行うことを特徴とする課金システムである。

【００１２】

請求項１９の発明は、配付された圧縮符号化および／または暗号化されたソフトウェアを復号するに際し、電子マネーまたは電子利用権を介して課金処理がな

されるようにした情報処理装置であって、

電子マネーまたは電子利用権のセキュリティチェックを行い、

セキュリティチェックの結果が正しくないときには、ソフトウェアの復号の停止、並びにセキュリティチェックの結果が正しくないことの通知の少なくとも一方を行うことを特徴とする情報処理装置である。

【００１３】

電子マネー、電子利用権において、定期的に、または非定期的に、発行元または管理者がセキュリティを変更する。それによって、電子マネー、電子利用権のセキュリティをより高くすることができる。

【００１４】

【発明の実施の形態】

以下、この発明を音楽配信システムＥＭＤ(Electronic Music Distribution)に適用した一実施形態について説明する。最初に図１を参照して音楽配信システムの概略について説明する。図１において、１０１が音楽コンテンツ供給事業者例えばレコード会社を示し、１０２がコンテンツサーバを示す。レコード会社１０１が音楽コンテンツの制作およびその配給を行う。また、音楽コンテンツに関しての圧縮符号化、暗号化、ウォーターマークの埋め込みもレコード会社１０１が行う。コンテンツサーバ１０２には、レコード会社１０１が制作したコンテンツが蓄積される。

【００１５】

１０３は、著作権管理機構を示す。例えばＪＡＳＲＡＣ（日本音楽著作権協会）は、著作権管理機構１０２の具体例である。レコード会社１０１は、著作権管理機構１０３に対して権利登録を行い、著作権管理機構１０３から著作権料を受け取る。

【００１６】

１０４が配信された音楽コンテンツの再生機能を有するユーザデバイスを示す。ユーザデバイス１０４は、配信された音楽コンテンツを再生すると共に、再生課金の処理を行う機能を有する。すなわち、暗号化を復号し、また、圧縮符号化を復号することによって、コンテンツを再生することができ、復号に対して課金

がされる。コンテンツサーバ１０２とユーザデバイス１０４との間には、必要に応じてコンテンツ配信事業者が介在し、ユーザに対してコンテンツサーバ１０２内のコンテンツを配信する。配信事業者が使用する配信手段としては、幾つかのものがある。その一つは、販売店１０５である。例えば雑誌の付録として、コンテンツが記録されたメディアが配付される。また、インターネット、ＣＡＴＶ(cable television)のような有線ネットワーク１０６がコンテンツの配信手段として使用される。さらに、携帯電話網１０７、衛星放送、衛星通信等の衛星ネットワーク１０８もコンテンツの配信手段として使用される。

【００１７】

この発明では、上述したコンテンツ配信手段として、有料で配信されるコンテンツの配信手段を利用することを妨げるものではない。媒体例えばＣＤ(Compact Disc;ＣＤ、登録商標）の場合には、記録されている楽曲に対しての著作権料がＣＤの価格に含まれている。配付を無料とし、復号（再生）に課金されるコンテンツをＣＤ上の有料コンテンツが記録された領域とは別の領域に記録するようにしても良い。

【００１８】

図１中では、販売店１０５が配付する媒体の一つとしての拡張ＣＤ１２１が示されている。拡張ＣＤ１２１の内周側の領域１２２は、既存のＣＤと同一のフォーマットで、配付が有料で、再生が無料とされた楽曲データが記録された領域である。また、外周側の領域１２３は、配付が無料で、再生が有料のコンテンツが記録された領域である。コンテンツは、圧縮符号化されているので、領域１２３が少なくても必要な長さの音楽データを記録することができる。

【００１９】

ＣＤ以外にMD、メモリカード等の媒体の場合にも、互いに区別できる領域として、配付が有料で、且つ再生が無料のコンテンツと、配付が無料で、且つ再生が有料のコンテンツとを記録することができる。また、衛星テレビジョン放送を利用して音楽コンテンツを配信するサービスを利用して配付が無料で、再生が有料のコンテンツを配信しても良い。

【００２０】

ユーザデバイス１０４は、コンテンツを無料で受け取ることができる。また、受け取ったコンテンツの再配付も自由に行うことができる。ここで、無料というのは、通信費、電気代等の実費を含まず、著作権料に関して無料という意味である。ユーザデバイス１０４が受け取ったコンテンツを再生、より具体的には、暗号化を復号する時に課金処理がなされる。課金処理のために、聴取権データ１０９が使用される。聴取権データ１０９は、ＩＣカード、セキュアデコーダ内のメモリに格納されている。聴取権データ１０９は、聴取権データ管理会社の管理下で、ユーザが所有する課金チャージャまたは最寄りの販売店に設置された販売端末によって書き換えることが可能とされている。聴取権データ１０９は、例えば再生可能な度数であり、ユーザデバイス１０４が課金の対象のコンテンツを再生する度に、度数が減算される。

【００２１】

なお、以下の説明では、聴取権データを例に説明するが、電子マネーをコンテンツの再生の支払いに当てることもできる。さらに、電子マネー、聴取権データ等を一括して扱うことができる多目的ＩＣカードを使用することもできる。

【００２２】

また、レコード会社１０１、著作権管理機構１０３、ユーザデバイス１０４と関係して代金決済のために、決済センター１１０が存在している。決済センター１１０は、認証／課金サーバ１１１を備えている。決済センター１１０は、銀行、クレジットカード会社２０８との間で、代金の決済を行う。

【００２３】

ユーザデバイス１０４が受け取ったコンテンツの再生を要求すると、認証／課金サーバ１１１に対してユーザデバイス１０４の認証を要求する（Ａ１の経路で示す）。ユーザデバイス１０４が正規のものであり、認証が成立すると、認証／課金サーバ１１１は、ユーザデバイス１０４に対して課金の要求を行う（経路Ａ２）。また、ユーザデバイス１０４は、決済センター１１０との間で、代金決済を行う（経路Ａ３）。

【００２４】

決済センター１１０は、認証／課金サーバ１１１に対して、経路Ａ４で示すように、課金がされたことまたは課金が可能であることを伝達すると共に、コンテンツサーバ１０２に対してコンテンツを要求する（経路Ａ５）。コンテンツサーバ１０２が認証／課金サーバ１１１に暗号化を復号するための鍵データを渡す（経路Ａ６）。認証／課金サーバ１１１がユーザデバイス１０４に対して、鍵データを渡す（経路Ａ７）。ユーザデバイス１０４は、この鍵データによって、コンテンツの暗号を復号化し、コンテンツを再生することができる。復号化がされることをもって、そのコンテンツの再生がされたものと判断され、聴取権データ１０９の度数が例えば－１される。度数が０に達すると、ユーザデバイス１０９が復号化ができなくなる。

【００２５】

図２は、聴取権データ１０９に関するシステムの一例を示し、音楽コンテンツの配付、コンテンツの暗号化の復号化のためのデータの授受については、省略されている。ユーザデバイス１０４に対応するものとして、プレーヤ２０１が示されている。プレーヤ２０１は、セキュアデコーダ２０２を内蔵している。また、プレーヤ２０１は、例えば携帯形オーディオ機器である。図２において、破線で示すように、プレーヤ２０１が再生する媒体（光ディスク、メモリカード等）には、音楽コンテンツが記録されている。音楽コンテンツの配信の方法は、図１に示したように、種々のものが使用できる。

【００２６】

２０４は、コーザ端末としての聴取権データチャージャを示す。データチャージャ２０４は、プレーヤ２０１のセキュアデコーダ２０２と決済センター１１０またはレコード店、コンビニエンスストア等に設置されているデータ販売端末２０６との間に存在して聴取権データ中継器として機能する。

【００２７】

図３は、データチャージャ２０４の機能を概略的に示すものである。図３において、家庭内に設置される可能性のあるプレーヤの具体例が示されている。５１がアンプとスピーカとが別体とされたオーディオ再生システムであり、５２がチ

ューナ、ＣＤプレーヤ（またはＭＤ（Mini Disc,登録商標）レコーダ）が一体化された再生機器であり、５３が携帯型ＣＤプレーヤであり、５４が携帯型ＭＤプレーヤであり、５５がパソコンである。これらのユーザデバイスには、ＩＣ構成のセキュアデコーダ５１ａ、５２ａ、５３ａ、５４ａ、５５ａが装備されている。これらのユーザデバイスに対して、データチャージャ２０４が共用され、専用接続線あるいは非接触無線通信、またはＵＳＢ(Universal Serial Bus)あるいはＩＥＥＥ(Institute of Electrical and Electronics Engineers) １３９４によって、聴取権データの送信と、再生履歴情報の吸い上げを行うことができる。データチャージャ２０４は、携帯可能な構成とされている。

【００２８】

プレーヤ２０１内のセキュアデコーダ２０２とデータチャージャ２０４とが有線または無線の通信路を介して通信を行い、聴取権データがデータチャージャ２０４からセキュアデコーダ２０２内のメモリに対して転送される。聴取権データは、例えばプレーヤ２０１の再生可能回数情報または再生可能時間に対応している。

【００２９】

また、プレーヤ２０１からデータチャージャ２０４に対して、有線または無線の通信路２０５を介してプレーヤ２０１の再生履歴情報（再生ログ）が伝送される。再生ログは、復号したディジタルデータの識別子および／または復号の条件を含む。具体的には、聴取した音楽コンテンツの種類、再生回数、再生時間等の情報を含んでいる。また、再生ログには、ユーザ端末の所有者、ユーザデバイスの識別子等の課金対象者を特定するための識別子が含まれている。セキュアデコーダ２０２とデータチャージャ２０４とは、必要に応じて認証を行い、認証が成立すると、暗号化された聴取権データおよび再生ログの伝送がなされる。

【００３０】

聴取権データは、決済センター１１０から通信路２０７例えば電話回線を介してデータチャージャ２０４に渡される。または、決済センター１１０から通信路２０９を介して販売端末２０６に渡された聴取権データが通信路２０５を介してデータチャージャ２０４に渡される。この場合にも、セキュリティの確保のため

に、認証と暗号化とがなされる。

【００３１】

データチャージャ２０４に吸い上げられた再生ログは、通信路２０７を介して決済センター１１０に送られる、または、通信路２０５を介して販売端末２０６に渡される。販売端末２０６は、通信路２０９を介して決済センター１１０から聴取権データを受け取ると共に、再生ログを決済センター１１０へ送る。さらに、入手した聴取権データの代金を決済センター１１０に支払う。通信路２０９は、電話回線、インターネット等である。

【００３２】

決済センター１１０と聴取権データチャージャ２０４との間では、通信路２０７を介して聴取権データおよび再生ログの送受信がなされる。この場合にも、セキュリティの確保のために、認証と暗号化とがなされる。聴取権データの決済に関して、銀行、クレジットカード会社２０８が存在している。銀行、クレジットカード会社２０８は、予め登録してあるユーザの銀行口座から決済センター１１０の依頼に基づいて、データチャージャ２０４に書き込んだ聴取権データ相当する金額を引き落とす。

【００３３】

さらに、決済センター１１０は、レコード会社１０１から聴取権データに関するサービスの管理の委託を受ける。また、決済センター１１０は、レコード会社１０１に対して聴取権データに関する技術の提供を行い、さらに、楽曲聴取料を支払う。レコード会社１０１は、図１を参照して説明したように、著作権管理機構１０３に対して著作権の登録を行うことによって、著作権の管理を依頼し、著作権管理機構１０３から著作権料を受け取る。

【００３４】

図２では省略しているが、聴取権データチャージャ２０４は、他のチャージャとの間で、通信装置例えば非接触通信装置を通じて、視聴権データの一部または全部を移動・合算・分割可能とされている。また、データチャージャ２０４は、プレーヤ２０１のセキュアデコーダ２０２以外にＩＣカードの構成のプリペイドカードに対して聴取権データを転送可能とされている。

【００３５】

図４は、図２に示される課金処理システムにおけるレコード会社１０１、決済センター１１０、聴取権データチャージャ２０４、聴取権データ販売端末２０６および銀行、クレジットカード会社２０８の相互の関係を抜き出したものである。決済センター１１０がチャージャ２０４および販売端末２０６との間で、聴取権データの販売を行い、また、再生ログを収拾し、それによって代金の決済を行う機能を有する。

【００３６】

図５は、聴取権データ端末２１０（聴取権データチャージャ２０４または販売端末２０６）と接続された決済センター１１０の機能をより詳細に示すものである。図５中で、実線の経路は、課金処理を実行する上で必要な処理を意味し、破線経路が課金処理を行う準備として必要な処理を意味する。多くの場合、破線の経路が郵送（文書の授受）によりなされ、実線の経路の処理がデータ通信でなされる。

【００３７】

最初に破線経路による処理について説明する。レコード会社１０１と決済センター１１０の間では、レコード会社１０１が決済センター１１０に対して業務委託登録を行う（ブロック２１１）。決済センター１１０は、レコード会社１１０に対してマーケティングデータを渡したり、各種報告を行う（ブロック２１２）

【００３８】

聴取権データチャージャ２０４の所有者である顧客２１３は、銀行、クレジットカード会社２０８との間で、料金の支払い、口座からの料金の引き落とし等の契約を結ぶ。顧客２１３が契約内容の変更等を決済センター１１０に連絡し、決済センター１１０が顧客情報の入力・修正を行う（ブロック２１４）。決済センター１１０が顧客２１３に対して請求書・領収書の発行とその郵送を行う（ブロック２１５）。

【００３９】

次に実線経路による処理について説明する。決済センター１１０が顧客の要求

に応じて聴取権データ端末２１０に対して聴取権データを送る。その場合、顧客の特定がなされ、また、通信サーバ２１６を介して認証・暗号化の処理がされたデータを送る。顧客管理システム２１７は、データベース２１８中の顧客情報を参照して、認証した顧客を特定する。そして、転送した聴取権データの量に基づいて、金融決済システム２１９に対して、料金の引き落としを依頼する。金融決済システム２１９が銀行、クレジットカード会社２０８に対して顧客の口座からの料金の支払いを依頼し、料金の支払いが実行される。支払いの完了の報告を決済センター１１０が受け取ると、顧客への領収書の発行がなされる。

【００４０】

聴取権データ端末２１０に対して、聴取権データを転送するのに先行して認証がなされる。そして、聴取権データ端末２１０から通信サーバ２１６を介して再生ログを決済センター１１０が受け取る。受け取った再生ログが通信サーバ２１６にて暗号化が復号され、再生ログ管理システム２２０へ送られる。再生ログには、顧客（聴取権データ端末２１０）を特定するための端末識別子と、復号・再生した音楽コンテンツを特定する識別子と、各音楽コンテンツを聴取した回数、時間、期間のデータとが含まれている。端末識別子は、主として上述したような聴取権データを転送したり、課金のために使用される。

【００４１】

再生ログ管理システム２２０が再生ログを一旦データベース２１８に格納し、予め決められた時、例えば1カ月毎にバッチ処理で再生ログまたは再生ログを処理したデータを聴取料決済システム２２１に渡す。聴取料決済システム２２１は、レコード会社１０１から業務委託時にデータベース２１８に登録した曲等の情報を参照して、曲毎の聴取料（著作権使用料）を算出する。曲以外に作曲家、作詞家、歌手、演奏者等の項目毎に聴取料を算出することも可能である。聴取料決済システム２２１が算出した曲毎の聴取料がレコード会社１０１に対して支払われる。

【００４２】

上述したように、決済センター１１０が顧客２１３への聴取権データの転送と聴取料の請求を行い、一方、決済センター１１０が曲毎の聴取料を算出し、分

配する処理を行うので、レコード会社１０１が顧客管理を行ったり、聴取料を算出したり、分配する業務を行う必要がない。また、決済センター１１０は、レコード会社１０１と独立した機関であるので、複数のレコード会社との間で業務委託の契約を行うことができ、顧客が選択できる音楽コンテンツの種類を豊富とすることができる。

【００４３】

図６は、セキュアデコーダ２０２を有するプレーヤ２０１の信号処理の構成を示す。セキュアデコーダ２０１は、破線で示すように、１チップのＩＣとして構成されたものである。また、セキュアデコーダ２０１は、所謂タンパーレジスタント(tamper resistant)の構成とされている。すなわち、外部からは、その内容が分からないような構成とされ、改ざんができない構成とされている。

【００４４】

媒体１には、圧縮符号化され、また、暗号化された音楽データが記録されている。さらに、再生課金処理に必要なデータが圧縮符号化、暗号化されたデータに付随している。圧縮符号化、暗号化されたデータをコンテンツデータと称し、再生課金処理のためのデータを付随データと称する。但し、この発明では、圧縮符号化と暗号化との両方が施されていることは、必ずしも必要ではない。圧縮符号化のみでも、その復号方法が非公開であれば、著作権保護の目的を果たすことが可能である。

【００４５】

媒体１としては、メモリカード、記録可能な光ディスク、読み出し専用の光ディスク等を使用できる。記録可能な媒体の場合では、上述したように、衛星ネットワーク、携帯電話ネットワーク、インターネット等のネットワークを介して配信されたデータをダウンロードすることができる。媒体１に記録されているコンテンツデータおよび付随データがインターフェース２を介してセキュアデコーダ２０２に供給される。セキュアデコーダ２０２からは、アナログオーディオ信号が出力される。アナログオーディオ信号は、アンプ等を介してスピーカ、ヘッドフォン等によって再生される。

【００４６】

セキュアデコーダ２０２は、暗号化の復号器１１と、圧縮符号化の伸長器１２と、Ｄ／Ａ変換器１３とを有している。暗号化としては、ＤＥＳ(Data Encryption Standard)を使用できる。ＤＥＳは、平文をブロック化し、ブロック毎に暗号変換を行うブロック暗号の一つである。ＤＥＳは、６４ビットの入力に対して６４ビット（５６ビットの鍵と８ビットのパリティ）のキーを用いて暗号変換を行い、６４ビットを出力する。ＤＥＳ以外の暗号化を使用しても良い。例えばＤＥＳは、暗号化と復号化に同一の鍵データを使う共通鍵方式であるが、暗号化と復号化に異なる鍵データを使う公開鍵暗号の一例であるＲＳＡ暗号を採用しても良い。鍵データは、上述したように、認証が成立したユーザデバイス１０４に対して渡される。

【００４７】

セキュアデコーダ２０２には、ＣＰＵを含む制御部１４と、制御部１４と外部のＣＰＵとの通信を行うためのＣＰＵインターフェース１５と、メモリ部１６と、聴取権データをプリペイドチャージャから受信し、再生ログをプリペイドチャージャに伝送するための通信部１７およびアンテナ１８とが設けられている。制御部１４は、復号器１１における復号の前段で分離された付随データを受け取り、復号化、伸長化を行うための制御を行う。

【００４８】

また、通信部１７およびアンテナ１８は、非接触で聴取権データチャージャとの間で通信を行うためのものである。この通信は、認証がされることを条件として、暗号化されたプロトコルを使用してなされる。データのみならず、電力をチャージャから受信可能とされているので、プレーヤ２０１全体の電源がオフであっても、聴取権データの受信と、再生ログの送信とを行うことができる。受け取った聴取権データは、メモリ部１６に格納される。さらに、プレーヤ２０１の再生ログもメモリ部１６に記憶される。メモリ部１６は、電源オフとされても、その記憶内容が保持される不揮発性メモリである。

【００４９】

なお、コピー出力が復号器１１からセキュアデコーダ２０２の外部に出力する

ことが可能とされている。出力するか否かは、制御部１４により制御される。出力されるコピー出力は、付随情報とコンテンツデータである。さらに、復号器１１および伸長器１２は、制御部１４の指示に基づいて、復号処理および伸長処理をそれぞれ省略する機能を有している。それによって、元々暗号化および圧縮符号化がされていないオーディオデータ（リニアＰＣＭ）を再生することが可能とされている。

【００５０】

プレーヤ２０１の全体の動作を制御するために、２１で示すシステムコントローラが備えられている。システムコントローラ２１は、ＣＰＵで構成され、セキュアデコーダ２０２内の制御部１４と通信を行うことによって、セキュアデコーダ２０２の動作を制御する。また，システムコントローラ２１とバスを介して操作部２２、ディスプレイ２３、メモリ部２４、モデム２５が接続されている。さらに、システムコントローラ２１が媒体１の再生動作、並びに媒体インターフェース２の動作を制御する。

【００５１】

操作部２２は、ユーザが操作するスイッチ、キー等であり、プレーヤ２０１の動作を制御する指示を発生する。ディスプレイ２３は、例えば液晶からなるもので、プレーヤ２０１の動作を制御するためのメニューを表示したり、動作状態を表示するために使用される。メモリ部２４は、システムコントローラ２１内のメモリの容量が少ないために設けられた外部メモリである。モデム２５は、公衆回線と接続され、外部とのデータの通信に使用される。例えば、セキュアデコーダ２０２のメモリ部１６内の再生ログをメモリ部２４に転送することによって、残りの再生可能回数または再生可能時間をディスプレイ２３に表示したり、再生ログをモデム２５を介して送信することが可能とされている。さらに、聴取権データをモデム２５を介して受信することも可能である。

【００５２】

ユーザが操作部２２を操作することによって、媒体１内の所望のコンテンツの再生を指示する。そのコンテンツが再生に関して無料のものであれば、セキュアデコーダ２０２を通ってアナログ出力が発生しても、メモリ部１６に格納されて

いる聴取権データが変更されない。若し、再生したコンテンツが再生課金の対象である場合には、メモリ部１６内の聴取権データが変更される。

【００５３】

課金処理としては、種々のタイプが可能である。課金処理としては、大きく分けて、買取型と、グロスに視聴料金をとるタイプと、セキュアデコーダで暗号の復号化を行うごとに視聴料金を課する度数タイプとがある。買取型は、一旦買い取った後では、再生処理に対して課金されないタイプである。グロスに視聴料金をとるタイプは、視聴料金をまとめて支払う月極めタイプ、視聴期間、視聴時間を限定するタイプ等である。

【００５４】

セキュアデコーダで暗号の復号化を行うごとに視聴料金を課す度数タイプとして、幾つかの形態が可能である。第１の形態は、予め設定された金額（プリペイドカード、電子マネー）または度数からコンテンツの再生処理の度に、金額または度数を減算するものである。残高または残り度数が不足する場合には、再生ができなくなる。第２の形態は、コンテンツの再生処理の度に、金額または度数が加算されるものである。予め設定した金額または度数に累積金額または累積度数が達すると、再生ができなくなる。第３の形態は、コンテンツの再生時間に応じて、度数または金額が加算または減算されるものである。

【００５５】

金額または度数は、一定のものであっても良く、また、コンテンツに応じて重み付けされたものでも良い。また、課金処理は、コンテンツの１タイトル（音楽の例では、１曲）またはコンテンツの複数タイトル（音楽の例では、アルバム）と対応して行われる。

【００５６】

また、コンテンツの再生処理の定義の方法としては、コンテンツ全体を再生した場合に、再生を行ったものとしても良いし、また、コンテンツの再生時間が所定時間以上の場合を再生を行ったものとしても良い。さらに、普及・流通を促進するためのプロモーション用のコンテンツの再生に対しては課金されない。また、課金の対象となるコンテンツであっても、例えばコンテンツの先頭部分例えば

先頭から１０秒間の再生を無料としたり、コンテンツのハイライト部分のみの再生を無料としても良い。このように、再生処理に対して課金されるコンテンツと、再生処理が無料のコンテンツとが混在する場合に、付随情報によって課金／無料が識別される。

【００５７】

付随情報は、コンテンツデータ（圧縮符号化および暗号化されたコンテンツ例えばオーディオデータ）の前に付加されたデータである。付随情報は、必要に応じて暗号化される。また、記録可能な媒体には、コンテンツデータの前に付加されて記録されるか、または媒体１のデータ管理用領域に記録される。読み出し専用の媒体の場合には、データ管理領域に付随情報が記録される。光ディスクの場合では、一般的にディスクの最内周側の領域に管理領域が設けられる。メモリカードの場合には、例えば音楽データの１曲を１ファイルとして扱うようにしたファイル管理データが規定される。

【００５８】

付随データには、課金されるコンテンツか、無料のコンテンツかを指示する課金識別子、並びに上述したような買取型、グロス型、度数型等の課金タイプを区別し、各課金タイプにおける課金条件を指示する再生条件ラベルが含まれる。一例として、買取型の場合では、買取価格のデータが再生条件ラベルに記述され、グロス型の再生回数を制限する場合では、再生回数のデータが再生条件ラベルに記述され、グロス型の再生期間を制限する場合では、再生期間のデータ（１日、１週間、１ヵ月等）が再生条件ラベルとして記述され、度数型の場合では、度数のデータ（１円／２分、１円／１分、１円／３０秒、・・・）が再生条件ラベルとして記述される。さらに、課金を前提としているコンテンツであっても、無料で視聴できる場合の条件を再生条件ラベルに記述することもできる。

【００５９】

また、付随情報中に、コンテンツデータの圧縮符号化の種類を示すための情報、暗号の種類および暗号のパラメータを示すための情報、チャンネル数の情報、ビットレートの情報等を記録しても良い。

【００６０】

さらに、付随情報中には、ＣＤ、ＭＤ、記録可能な光ディスク、不揮発性メモリを含むメモリカード等の媒体を一意に識別可能とするためのメディアＩＤ例えばシリアル番号が含まれる。さらに、付随情報中には、デコーダＩＤが配置される。デコーダＩＤは、ユーザの端末、ユーザのプレーヤ等に内蔵されているセキュアデコーダを一意に識別可能とするためのＩＤ例えばシリアル番号である。

【００６１】

次に、図７のフローチャートを参照してプレーヤ２０１（図６参照）においてなされる課金処理の一例について説明する。この処理は、セキュアデコーダ２０２内の制御部１４およびシステムコントローラ２１によってなされるものである。最初のステップＳ１は、媒体１に再生しようとするコンテンツが存在しているような再生スタンバイ状態である。具体的には、ＥＭＤにより配信されたコンテンツが媒体１に格納されている場合、媒体１に既にコンテンツが記録されている場合等が再生スタンバイに該当する。ステップＳ２では、ユーザが操作部２２の再生ボタンを押すことによって再生指示がされたかどうかが決定される。

【００６２】

ステップＳ２の結果が否定であることは、コピーの操作を意味するものとされている。ステップＳ３において、無料再生用コンテンツのコピーか否かが決定される。無料再生用コンテンツとは、再生が課金されないコンテンツを意味する。付随情報中に含まれる識別子を参照してステップＳ３の決定がなされる。無料再生用コンテンツであれば、著作権保護のために、セキュアデコーダ２０２からの暗号が復号化されたコピー出力が禁止される（ステップＳ４）。

【００６３】

若し、無料再生用コンテンツのコピーでない、すなわち、課金再生用コンテンツのコピーであるとステップＳ３で決定されると、課金再生用コンテンツのコピーがセキュアデコーダ２０２から出力される（ステップＳ５）。課金再生用コンテンツのコピーは、自由になされる。但し、このコピー出力は、付随情報と暗号化、圧縮符号化がされたデータである。

【００６４】

ステップＳ２において、再生動作が指示されたものと決定されると、ステップＳ６において、課金処理を受け入れるか否かが問われる。例えばプレーヤ２０１のディスプレイ２３にメッセージが表示され、ユーザが操作部２２の操作によって回答するようになされる。ユーザが課金処理を受け入れない場合には、無料再生ができない（ステップＳ７）。但し、再生条件ラベルによって指示される部分的無料再生例えば曲の先頭部分またはハイライト部分の再生を無料で行うことが許される場合もある。課金処理を受け入れる場合には、ステップＳ８において、ディスプレイ２３上に、現に再生しようとするコンテンツに関する再生課金条件が提示される。付随情報中の再生条件ラベルの情報に基づいて課金条件の提示がなされる。

【００６５】

ステップＳ９では、課金タイプが買取型かどうかが決定される。買取型であれば、買取用の課金がなされる（ステップＳ１０）。そして、ステップＳ１１において、セキュアデコーダ２０２の復号器１１では、鍵を使用して暗号を復号化し、ステップＳ１２において、無料再生を行う。この場合、無料再生するコンテンツのコピーが禁止される。但し、ムーブ、すなわち、コピーと異なり元のデータが残らない処理は、可能である。

【００６６】

ステップＳ９において、買取型でないと決定されると、ステップＳ１３においてグロス型例えば月極型かどうかが決定される。月極契約が存在しているときには、ステップＳ１４において、契約された楽曲か否かが決定される。そうであれば、ステップＳ１５において、無料再生がなされる。課金再生用コンテンツのコピーは自由に行うことができる。

【００６７】

ステップＳ１３において、月極型でないと決定されると、そのコンテンツは、度数型で課金されるものと決定される。そして、ステップＳ１７において、暗号の復号化がなされ、ステップＳ１８において、課金再生がなされる。課金再生では、上述したように、再生の度数、再生時間等に応じて課金される。また、課金

再生用コンテンツのコピーは、自由にできる。さらに、ステップＳ１４において、月極契約の範囲内でないと決定された場合も、課金再生の処理（ステップＳ１７、ステップＳ１８）がなされる。

【００６８】

図８は、聴取権データチャージャ２０４の一例の構成を示す。チャージャ２０４は、例えば持ち運び可能な可搬型の構成とされている。３０１がチャージャ全体を制御するＣＰＵを示し、３０２が暗号化・復号化モジュールを示し、３０３がディスプレイ（例えば液晶ディスプレイ）を示し、３０４がユーザによって操作されるキー・ボタンを示す。ディスプレイ３０３には、チャージャの動作に関連するメニュー、課金処理条件等が表示される。暗号化・復号化モジュール３０２は、再生ログ等の送信時の暗号化の処理と、聴取権データ等の受信時の暗号の復号化の処理とを行う。３０５は、データチャージャ個別ＩＤを示す。データチャージャ個別ＩＤ３０５は、例えば再生ログと共に決済センターへ送信され、データチャージャと再生ログの対応関係が分かるようになされる。

【００６９】

また、決済センター（図２中の決済センター１１０）との通信のために、モデム３０６およびＵＳＢ(Universal Serial Bus)通信モジュール３０７が設けられている。モデム３０６によって、電話回線を介して決済センターとの通信が行われ、決済センターから聴取権データを受け取り、また、決済センターに対して再生ログを送信することができる。ＵＳＢ通信モジュール３０７を使用し、パーソナルコンピュータおよびインターネットによって同様に決済センターとの通信が可能である。

【００７０】

決済センターからデータチャージャ２０４が受信した聴取権データが聴取権データメモリ３０８に格納される。また、プレーヤ２０１のセキュアデコーダ２０２から受け取った再生ログが使用状況メモリ３０９に格納される。必要に応じてチャージャ２０４のログが再生ログに付加されたログデータが決済センターへ送信される。メモリ３０８および３０９は、電源オフとされても、その記憶内容が保持される不揮発性メモリである。

【００７１】

また、非接触通信モジュール３１０およびアンテナ３１１は、非接触でプレーヤ２０１との間で通信を行うためのものである。この通信は、認証がされることを条件として、暗号化されたプロトコルを使用してなされる。データのみならず、セキュアデコーダ２０２が動作するのに必要な電力をプレーヤに送信可能とされている。したがって、プレーヤ２０２のメインの電源がオフであっても、聴取権データおよび再生ログの授受が可能とされている。アンテナ３１１以外にライン接続用の端子も備えられている。なお、非接触通信モジュール３１０およびアンテナ３１１またはラインを使用して聴取権データ販売端末２０６との通信を行うようになされる。

【００７２】

図９は、セキュアデコーダ２０２のより詳細な構成、すなわち、課金処理に関する機能的構成を示す。図８に示される構成要素と対応する部分には、同一符号を付して示す。媒体１からの暗号化され、且つ圧縮符号化されたコンテンツデータと付随データとからなる再生データが復号器１１に供給される。復号器１１には、媒体１を一意に識別可能とするためのメディア個別ＩＤも供給される。復号器１１によって暗号の復号がなされる。

【００７３】

復号器１１の出力データが再生条件ラベル検出部４０１に供給され、付随データ中の再生条件ラベルが検出される。検出された再生条件ラベルがセキュアデコーダ２０２の処理に使用される。伸長器１２では、圧縮符号化の復号がなされる。伸長器１２の出力データがウォーターマーク検出部４０２に供給される。ウォーターマーク検出部４０２は、アナログ出力時に付加したウォーターマークを検出し、検出されたウォーターマークと再生条件ラベルとに基づいて、再生条件ラベルが改ざんされたか否かをチェックする。

【００７４】

４０３は、聴取権カウンタを示す。聴取権カウンタ４０３においては、再生データを復号する度に、聴取権データに対して変更を加える。例えばメモリ部１６に格納されている聴取権データ例えば度数データを減算する処理を行う。メモリ

部１６に格納される聴取権データは、アンテナ１８（またはライン）と通信モジュール１７とによって、上述した聴取権データチャージャ２０４から送信されたものである。通信モジュール１７内には、再生ログ等の送信時の暗号化と、聴取権データの受け取り時の復号化のためのモジュールが設けられている。なお、ここでは、楽曲データを取り扱うために、聴取権の用語を使用しているが、映像データを含めて考えた時には、聴取権の代わりに視聴権の用語が使用される。

【００７５】

聴取権カウンタ４０４において、聴取権に関する処理がされると、ウォーターマーク付加部４０４において、出力されるデータに対してウォーターマークが付加される。ウォーターマークは、楽曲データに存在する冗長な部分例えば出力されるオーディオデータの下位のビットを利用することでウォーターマークを付加できる。付加されたウォーターマークは、アナログ信号に変換しても残り、且つウォーターマークを除去することが不可能か、非常に困難なものである。付加されるウォーターマークは、再生条件ラベルの全体または一部のデータと、デコーダ個別ＩＤ４０５の情報を含むものである。ウォーターマークが付加されたデータがＤ／Ａ変換器１３によってアナログ出力に変換され、セキュアデコーダ２０２の外部へ出力される。上述したウォーターマーク検出部４０２は、このように付加されたウォーターマークを検出するものである。

【００７６】

セキュアデコーダ２０２がＩＣカードのインターフェースを持ち、また、聴取権データチャージャ２０４が決済センターまたは金融会社から電子マネーを受け取り、受け取った電子マネーをセキュアデコーダ２０２が備えているインターフェースを介してＩＣカードに記録するようにしても良い。すなわち、聴取権データの書き込みに対して、オプショナルなものとして電子マネーの記録装置としての機能を持たせることができる。

【００７７】

聴取権カウンタ４０３によってなされる課金処理の概略を説明する。一例として、課金処理が度数型で行われる場合に適用される例について説明する。すなわち、予め設定された度数から楽曲データの再生処理の度に、度数を減算したり、

楽曲データの再生処理の度に、度数が加算されたり、楽曲データの再生時間に応じて、度数が加算または減算される。再生データ例えば楽曲データから再生条件ラベル検出部４０１が再生条件ラベルを抜き出す。再生条件ラベルには、課金条件が含まれている。また、楽曲データが伸長器１２から出力されている期間を３０秒、１分等の単位時間によって計測し、計測された時間の長さに対して課金される。すなわち、単位時間が一つの度数に対応される。

【００７８】

計測された時間と再生条件ラベルに基づいて、聴取権カウンタ４０３によって度数が制御される。すなわち、再生条件ラベルを参照して、メモリ部１６に格納されている聴取権データに対して減算または加算処理を行い、聴取権データを書き換える。また、再生時間または再生期間を再生条件としている場合には、タイマー／カレンダーに対して、再生時間の累積処理または現在日時と再生可能期限との照合処理がなされる。

【００７９】

聴取権カウンタ４０３または他の制御部は、さらに、再生可能かどうかを判断する。例えば再生した度数を減算して、残りが０となると、再生不可能と判断する。また、累積度数が設定された度数に到達したり、再生時間の累積が設定された時間に到達したり、現在の日時が再生期限を越えたりすると、同様に、再生不可能と判断する。再生可能な場合には、楽曲データが出力され、一方、再生不可能な場合には、楽曲データの出力が禁止される。

【００８０】

この発明の一実施形態では、上述した決済センター１１０または聴取権データ販売機２０６から聴取権データチャージャ２０４に聴取権データを渡す場合、並びに聴取権データチャージャ２０４からプレーヤ２０１に聴取権データを渡す場合において、セキュリティを高くするために、発行元または管理者である決済センター１１０がセキュリティを定期的または非定期で変更可能とするものである。

【００８１】

図１０は、聴取権データを渡す時のデータフォーマットの一例を示す。図１０

Ａが１フレーム（２５６ビット）の構成を示す。フレームの先頭にヘッダ（１６ビット）が位置する。次に、開始年月日（ＹＭＤ）（２４ビット）と終了年月日（ＹＭＤ）とが順に配置される。聴取権データの有効な期間がこれらのデータによって規定される。年が１５ビットのバイナリ表記で表され、月および日がそれぞれ４ビットおよび５ビットのバイナリ表記で表される。開始日または終了日を決めていない場合には、２４ビットを全て０のビットとする。聴取権データの有効期間を予め定めておくことによって、終了年月日を明示しなくても良い。

【００８２】

続いて６ビットのタイプが暗号化の種類を表す。ＤＥＳ(Data Encryption Standard)による暗号化、ＲＳＡによる暗号化等が使用できる。ＤＥＳは、平文をブロック化し、ブロック毎に暗号変換を行うブロック暗号の一つである。ＤＥＳは、６４ビットの入力に対して６４ビット（５６ビットの鍵と８ビットのパリティ）のキーを用いて暗号変換を行い、６４ビットを出力する。ＤＥＳは、暗号化と復号化に同一の鍵データを使う共通鍵方式であり、ＲＳＡは、暗号化と復号化に異なる鍵データを使う公開鍵暗号の一つである。これら以外の暗号を使用することもできる。

【００８３】

暗号化の種類の情報の後に、１０ビットの鍵長が配される。鍵長は、暗号化を復号するための鍵の長さを示す。鍵長の後に鍵（図１０Ａの例では、１０２４ビット）が配置される。そして、３２ビットのＥＤＣ（エラー検出コード）用の鍵と、それに続いて２５６ビットの暗号化された聴取権データＭＰが配される。

【００８４】

データＭＰの後に６４ビットのＥＤＣと１２８ビットのＥＣＣ（エラー訂正コード）とが順に配置され、１フレームのデータ配置が完結する。ＥＤＣとして、ＣＲＣ（cyclic redundancy code）等が使用され、ＥＣＣとして、例えば（１９８，１８２，１７）のリードソロモンコード(Reed-Solomon code)が使用される。ＥＣＣは、ヘッダから始まり、ＥＤＣまでのデータのエラーの有無を検出する。ＥＤＣは、開始ＹＭＤから始まってデータＭＰまでのエラーを訂正する。

【００８５】

ＥＤＣの多項式として、例えば（$x^{16}+x^{12}+x^{5}+x+1$）（$x^{16}+x+1$）（$x^{32}+\_x^{31}+\_x^{30}\cdots+\_x^{4}+\_x^{3}+\_x^{2}+\_x+1$）を使用する時に、下線部分の係数の値がＥＤＣ用鍵（６４ビット）に配されている。したがって、データＭＰの暗号化を復号するためには、ＥＣＣによるエラー訂正を行い、ＥＤＣ用の鍵を得、次に、ＥＤＣによるエラー検出を行い、エラー検出の結果がＯＫ（エラー無し）であれば、データＭＰを復号できる。このようにして、暗号化された聴取権データＭＰのセキュリティを高くすることができる。さらに、必要に応じて、全体的にスクランブル（例えば最大長周期（Ｍ）系列を使用したランダム化）を行うようにしても良い。

【００８６】

図１０Ｂは、聴取権データの送信のための他のデータ構成例を示す。図１０Ａに示すデータ配列（影を付けて示す）の後に暗号化を行うためのソフトウェア（例えば４Ｍビット）が配され、さらに、暗号化のソフトウェアに対するＥＤＣソフトウェア（例えば１Ｍビット）が配される。ＥＤＣソフトウェアは、例えば２Ｋバイト単位でＥＣＣブロック化されている。図１０Ｂのデータ構成は、暗号化の復号用ソフトウェアも一緒に送るようにしたものである。

【００８７】

上述した聴取権データの伝送フォーマットは、重要な部分が２５６ビットのみであるが、その部分が暗号化、ＥＤＣ、ＥＣＣにより守られている。それによって、聴取権データを不正に入手したり、改ざんすることを防止できる。さらに、この発明の一実施形態では、図１０Ａに示すフォーマットにおける開始ＹＭＤ、鍵長、鍵、ＥＤＣ用鍵の内の少なくとも１つを決済センター１１０が定期的に、或いは非定期的に変更可能としている。それによって、聴取権データが改ざんされたり、不正利用される疑いがある時、またはこれらを未然に防ぐことができる。例えば聴取権データの暗号化の解読方法がインターネット上で公開されるような事態にも直ちに対処することができる。また、図１０Ｂに示すフォーマットでは、さらに、暗号化ソフトウェアおよび／またはＥＤＣソフトウェアを変更することができるので、セキュリティを強力とすることができる。

【００８８】

このように、聴取権データのセキュリティを変更した後では、旧いセキュリティの聴取権データが無効となり、旧い聴取権データでは、コンテンツを利用できないようになされる。この場合、使えなくなった旧い聴取権データを所有している者は、旧い聴取権データを新たな聴取権データへ交換すること決済センター１０に要求することができる。この交換システムの代わり、またはこのシステムに加えて、ユーザが聴取権データを使い切ったために、聴取権データを入手する時に、残っている旧い聴取権データが新しい聴取権データに自動的に交換されるシステムが採用される。

【００８９】

図１１は、コンテンツの再生と聴取権データのセキュリティとが連携した処理を示すフローチャートである。一例として、聴取権データのセキュリティが１年に１回定期的に変更される。ステップＳ１において、暗号化コンテンツの再生を行おうとすると、聴取権データが１年以内かどうかがステップＳ２で決定される。セキュアデコーダがカレンダーを内蔵しており、ステップＳ２の決定を行うことができる。この場合、１年に対してある程度の周知期間αを付加し、１年＋αを経過した時に聴取権データを無効とするようにしても良い。

【００９０】

１年以上経過している場合には、コンテンツの再生が停止する（ステップＳ３）。１年以内の聴取権データの場合には、聴取権データが最低単位（ａ）以上かどうかがステップＳ４で決定される。最低単位の聴取権データが残っていない場合には、再生が停止し、その旨のメッセージが提示される（ステップＳ５）。音声のメッセージを発生しても良い。また、ステップＳ３においても同様に、メッセージを提示するようにしても良い。

【００９１】

ステップＳ４において、聴取権データが最低単位ａ以上残っていると決定されると、聴取権データの１単位が消費される。聴取権データが実際に消費されたかどうかがステップＳ６において監視される。例えば、聴取権データの消費する前の状態と、消費した後の状態とが比較される。若し、不正な改ざん等によって、

聴取権データが消費されないときは、ステップＳ５の再生停止、メッセージの提示に移行する。ステップＳ６において、聴取権データの消費が確認できると、ステップＳ７において、コンテンツの暗号が復号され、コンテンツが再生される。再生の停止、メッセージの提示と共に、またはこれらの処理に代えて、決済センター１１０に対して、聴取権データのセキュリティチェックの結果が正しくないことを通知するようにしても良い。

【００９２】

コンテンツの再生が終了したかどうかがステップＳ８において決定される。再生の終了は、通常は、ユーザが再生の停止指示を行うことでなされる。再生が継続する限り、ステップＳ４～Ｓ８の処理が繰り返される。例えばユーザがコンテンツを再生している時間に応じて、聴取権データが消費される。そして、ステップＳ８において、再生が終了したものと決定されると、再生が終了する（ステップＳ９）。

【００９３】

図１１の例は、再生時間の単位時間に応じて聴取権データが減少する課金処理であるが、前述したような再生時間に応じて度数が加算される場合でも、同様にこの発明を適用できる。

【００９４】

また、利用しようとするコンテンツ例えば楽曲データが付随する情報中に年月日データ持ち、楽曲データと聴取権データとの間で、年月日データを照合し、聴取権データの年月日に応じて再生可能なコンテンツを識別することもできる。

【００９５】

さらに、新旧の聴取権データの入れ替えを行うようにしても良い。例えば１０００度数（ポイント）が入るデータチャージャの場合で、残りが３０００度数で、５０００度数を補充して欲しい時に、残りを含めた（３０００＋５０００）度数を新たな聴取権データとするようにしても良い。よりさらに、再生ログを伝送するシステムにおいては、不正に聴取を行っても、再生ログが許容量を越えると、再生を禁止するようにできる。そのような事態が生じた時に、決済センターに連絡がなされ、その連絡時に、残っている聴取権データを吸い上げるように

しても良い。よりさらに、再生ログを収集するシステムでは、電子マネー、電子利用権を送信した履歴と、再生ログの使用履歴とを比較することによって、不正を発見するようにしても良い。

【００９６】

なお、上述した実施形態では、主としてオーディオコンテンツについて説明したが、オーディオ以外のビデオデータ、静止画像データ、文字データ、コンピュータグラフィックデータ、ゲームソフトウェア、およびコンピュータプログラム等のコンテンツに対しても、上述したのと同様にこの発明を適用することができる。

【００９７】

【発明の効果】

以上の説明から明らかなように、この発明によれば、セキュリティを変更するので、電子マネー、電子利用権のセキュリティを向上することができる。例えば偽造の電子マネー、電子利用権が出回ったり、不正利用方法が公開されたりしても、直ちに対応することができる。また、定期的にセキュリティを変更することによって、不正利用、偽造のおそれを未然に防ぐことができる。さらに、セキュリティチェックの結果が正しくない時には、コンテンツの利用を禁止することで、電子マネー、電子利用権のみならず、コンテンツの著作権を強力に保護することができる。よりさらに、再生ログを収集するシステムでは、渡した電子マネー、電子利用権と再生ログから不正を発見することができる。

【図面の簡単な説明】

【図１】

この発明の一実施形態のシステム全体の概略を示すブロック図である。

【図２】

この発明の一実施形態における聴取権データに関する説明のためのブロック図である。

【図３】

この発明の一実施形態における聴取権データチャージャに関する説明のためのブロック図である。

【図４】

この発明の一実施形態における聴取権データに関する説明のためのブロック図である。

【図５】

この発明の一実施形態における決済センターの果たす機能に関する説明のためのブロック図である。

【図６】

この発明の一実施形態におけるプレーヤの一例のブロック図である。

【図７】

この発明の一実施形態における課金処理の一例を説明するためのフローチャートである。

【図８】

この発明の一実施形態における聴取権データチャージャの一例のブロック図である。

【図９】

この発明の一実施形態におけるセキュアデコーダのより詳細なブロック図である。

【図１０】

この発明の一実施形態における聴取権データのデータ構成の一例の略線図である。

【図１１】

この発明の一実施形態における聴取権データのセキュリティチェックとコンテンツ再生との関連する処理を説明するためのフローチャートである。

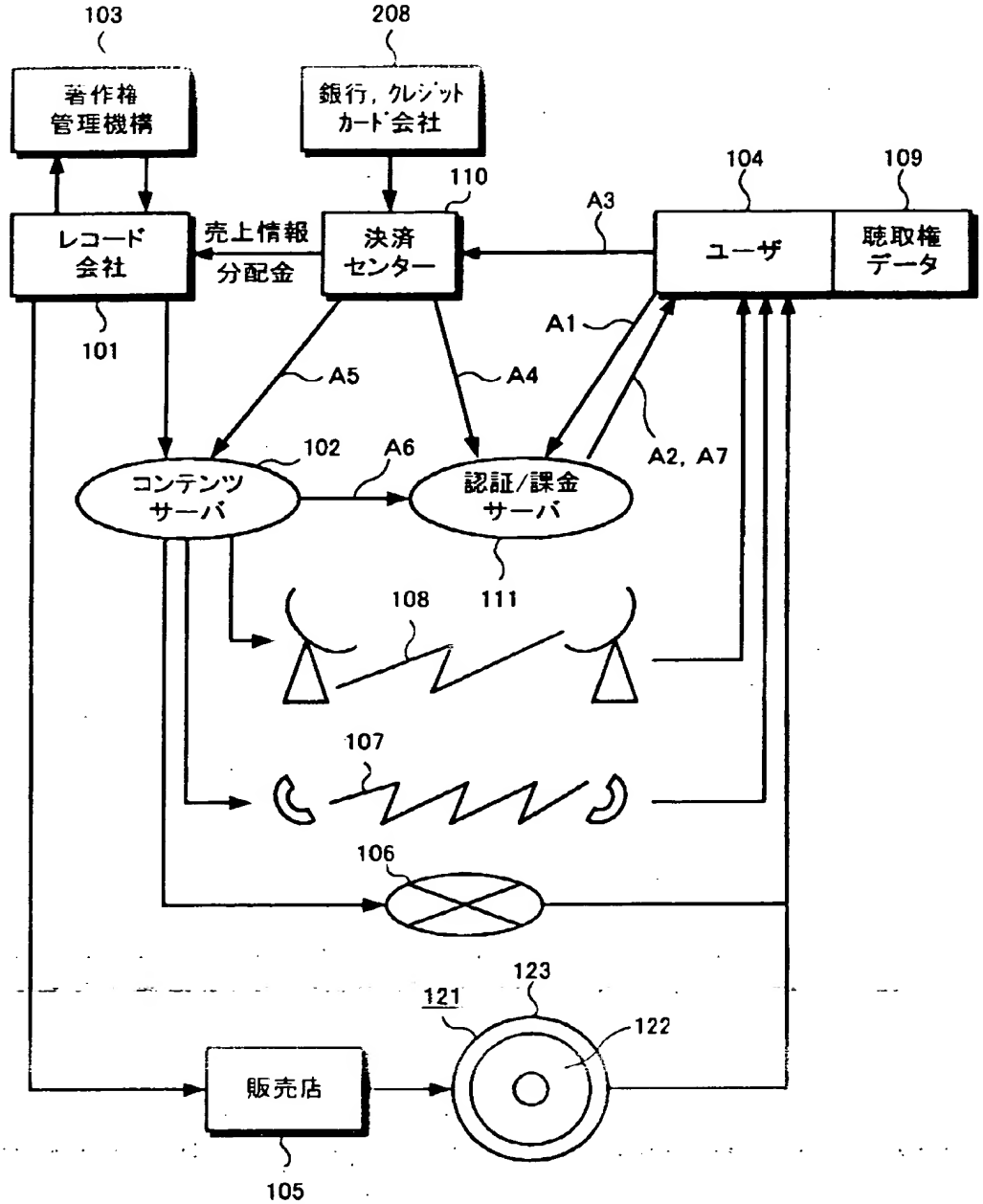
【符号の説明】

１・・・コンテンツの格納された媒体、１１・・・暗号化の復号器、１２・・・圧縮符号化の伸長器、２１・・・システムコントローラ、１０１・・・レコード会社、１０３・・・著作権管理機構、１０４・・・ユーザデバイス、１０９・・・聴取権データ、１１０・・・決済センター、２０１・・・プレーヤ、２０２・・・セキュアデコーダ、２０４・・・聴取権データチャージャ

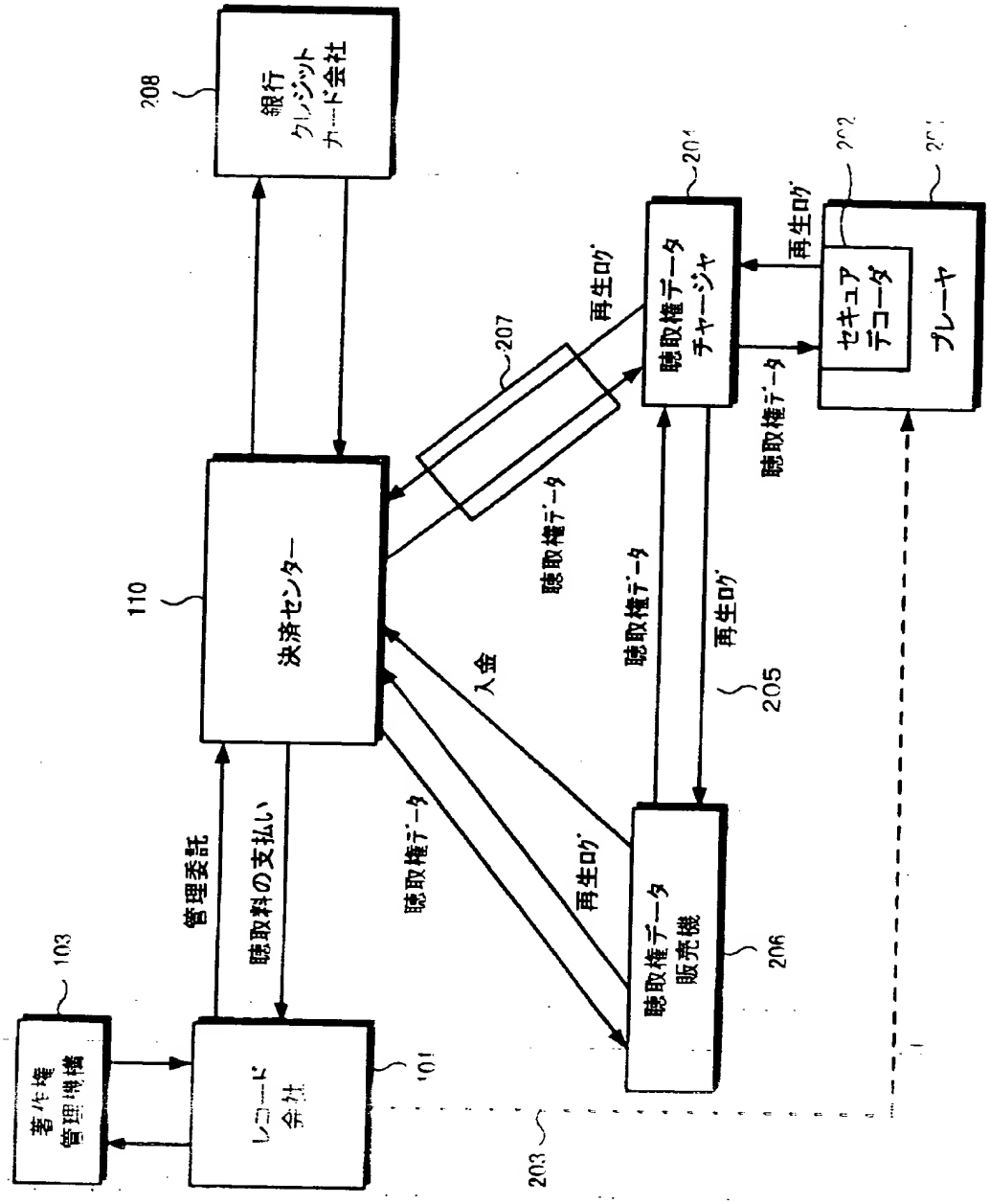
出証特２０００－３０７５４７９

【書類名】　図面

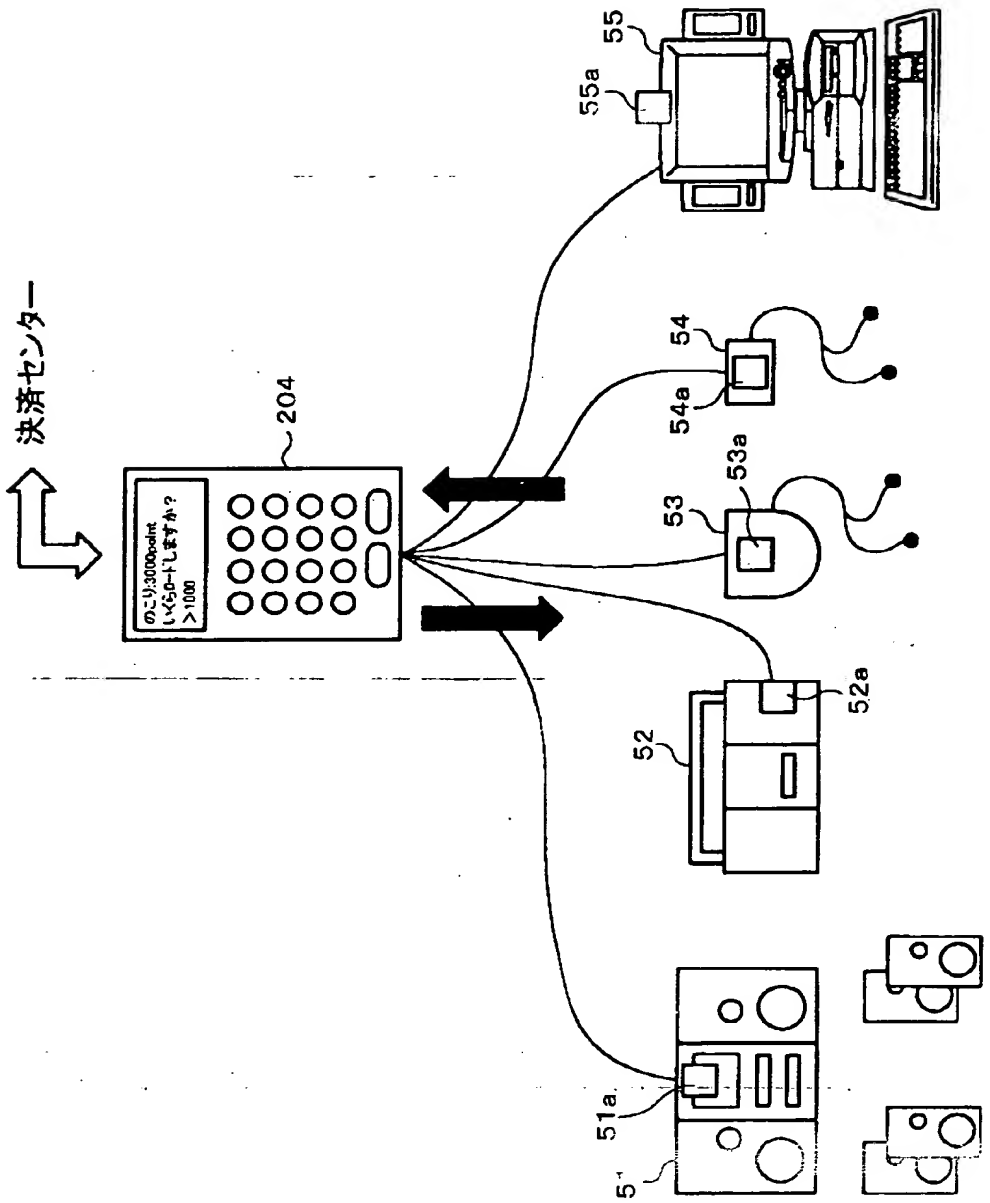
【図１】


103
208
著作権
管理機構
銀行，クレジット
カード会社
104
109
110
A3
レコード
会社
売上情報
分配金
決済
センター
ユーザ
聴取権
データ
101
A1
A5
A4
102
A6
A2，A7
コンテンツ
サーバ
認証/課金
サーバ
108
111
107
106
123
121
122
販売店
105

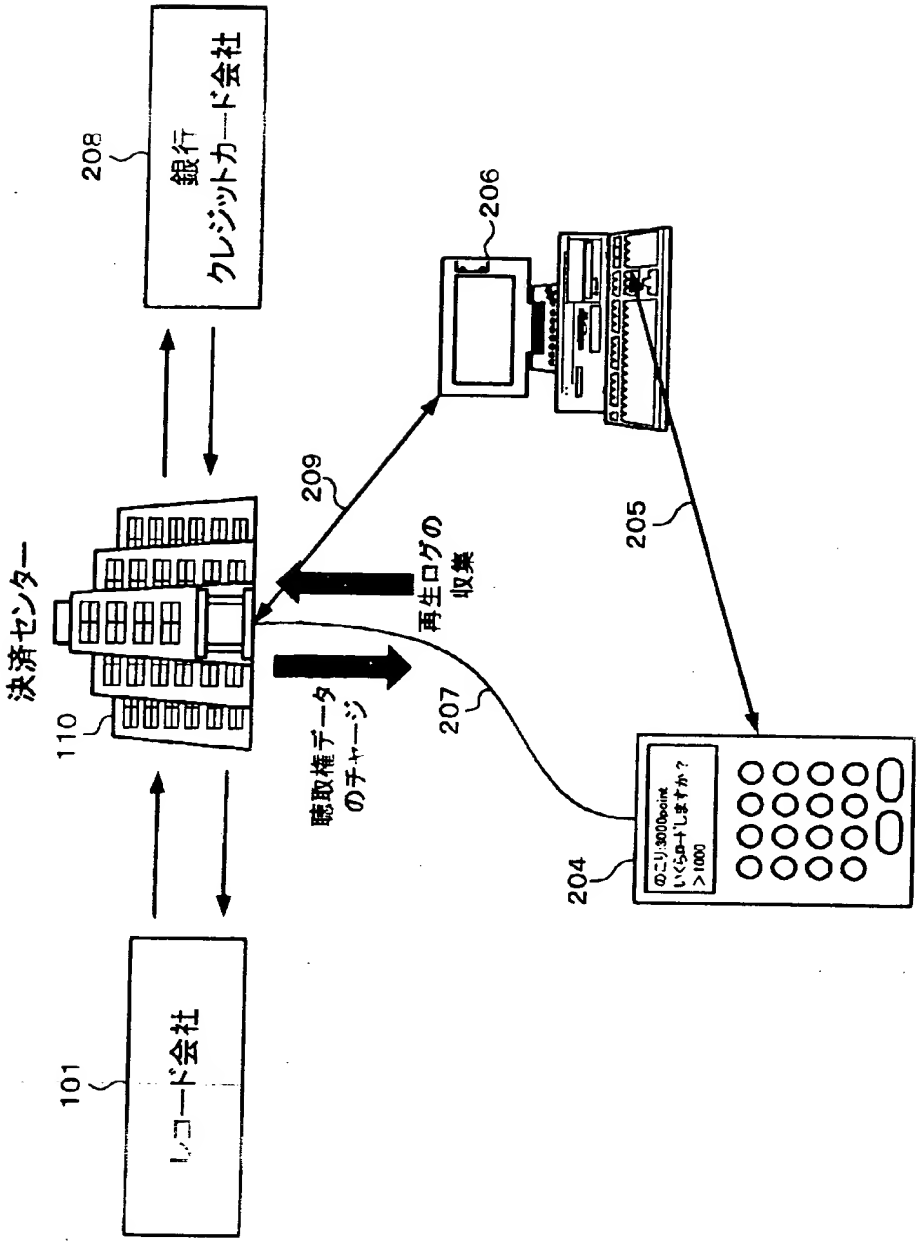
【図２】


銀行
クレジット
カード会社
208
決済センター
110
聴取権データ
チャージャ
再生ログ
セキュア
デコーダ
プレーヤ
聴取権データ
聴取権データ
再生ログ
205
聴取権データ
販売機
206
再生ログ
入金
聴取権データ
管理委託
聴取料の支払い
103
101
203
207

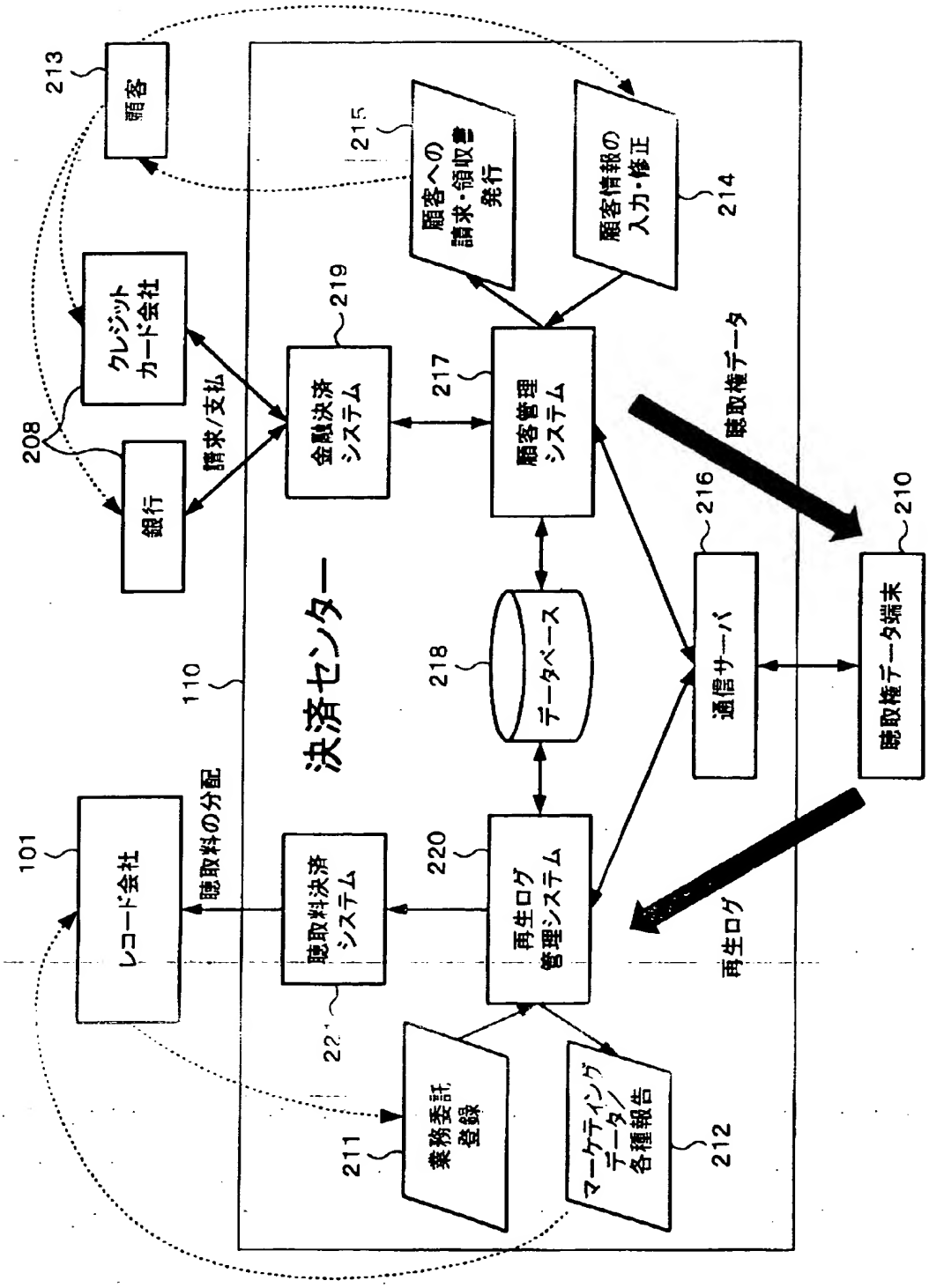
【図３】


決済センター
204
のこり3000point
いくらポートしますか？
>1000
55
55a
54
54a
53
53a
52
52a
51
51a
5'

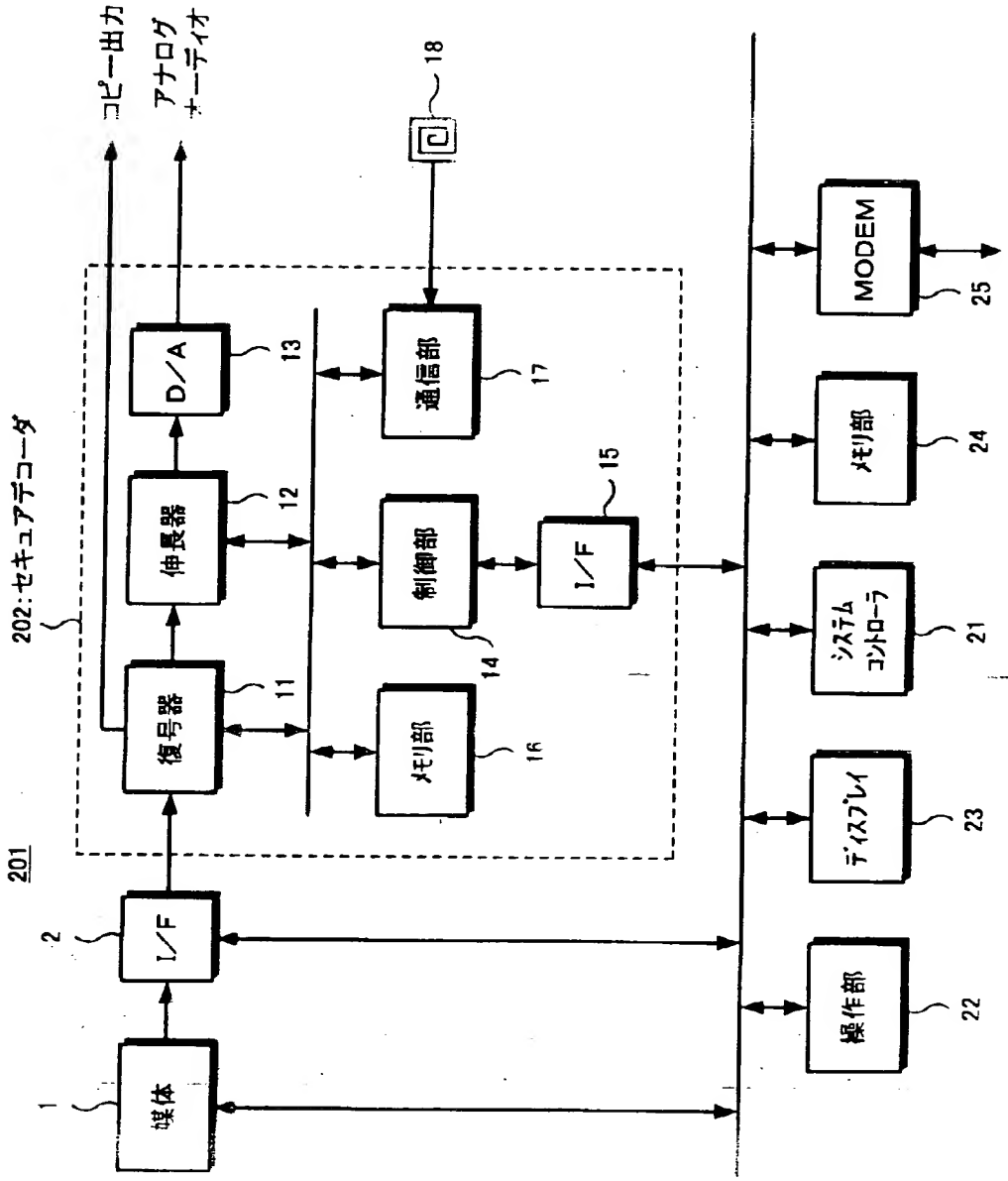
【図４】


銀行
クレジットカード会社
208
206
209
205
再生ログの
収集
決済センター
110
207
聴取権データ
のチャージ
204
のこり3000point
いくらロードしますか？
＞1000
レコード会社
101

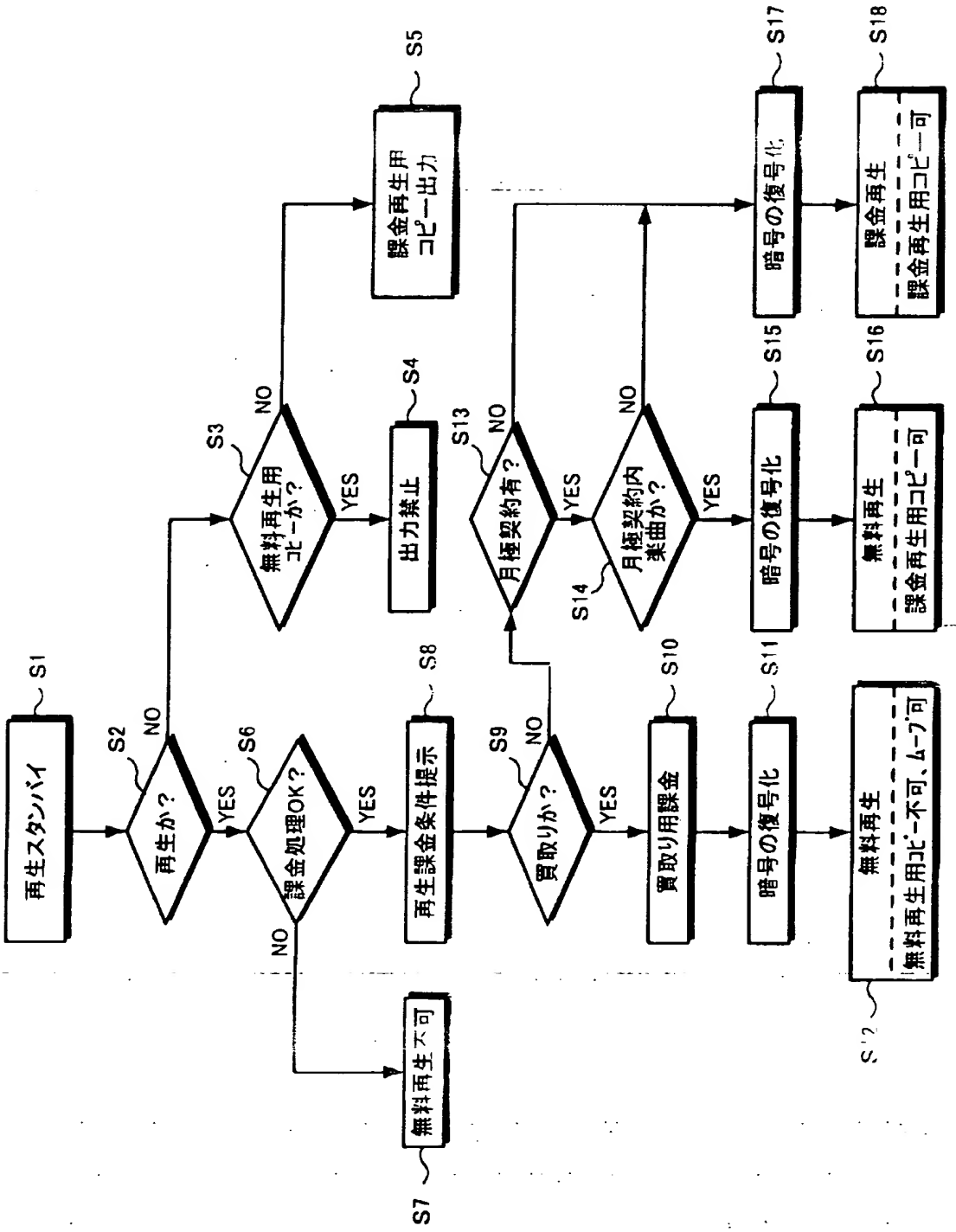
【図５】


213
顧客
215
顧客への請求・領収書発行
214
顧客情報の入力・修正
クレジットカード会社
219
金融決済システム
217
顧客管理システム
208
銀行
請求/支払
聴取権データ
216
210
決済センター
110
218
データベース
通信サーバ
聴取権データ端末
101
レコード会社
聴取料の分配
聴取料決済システム
220
再生ログ管理システム
再生ログ
211
業務委託登録
212
マーケティングデータ/各種報告

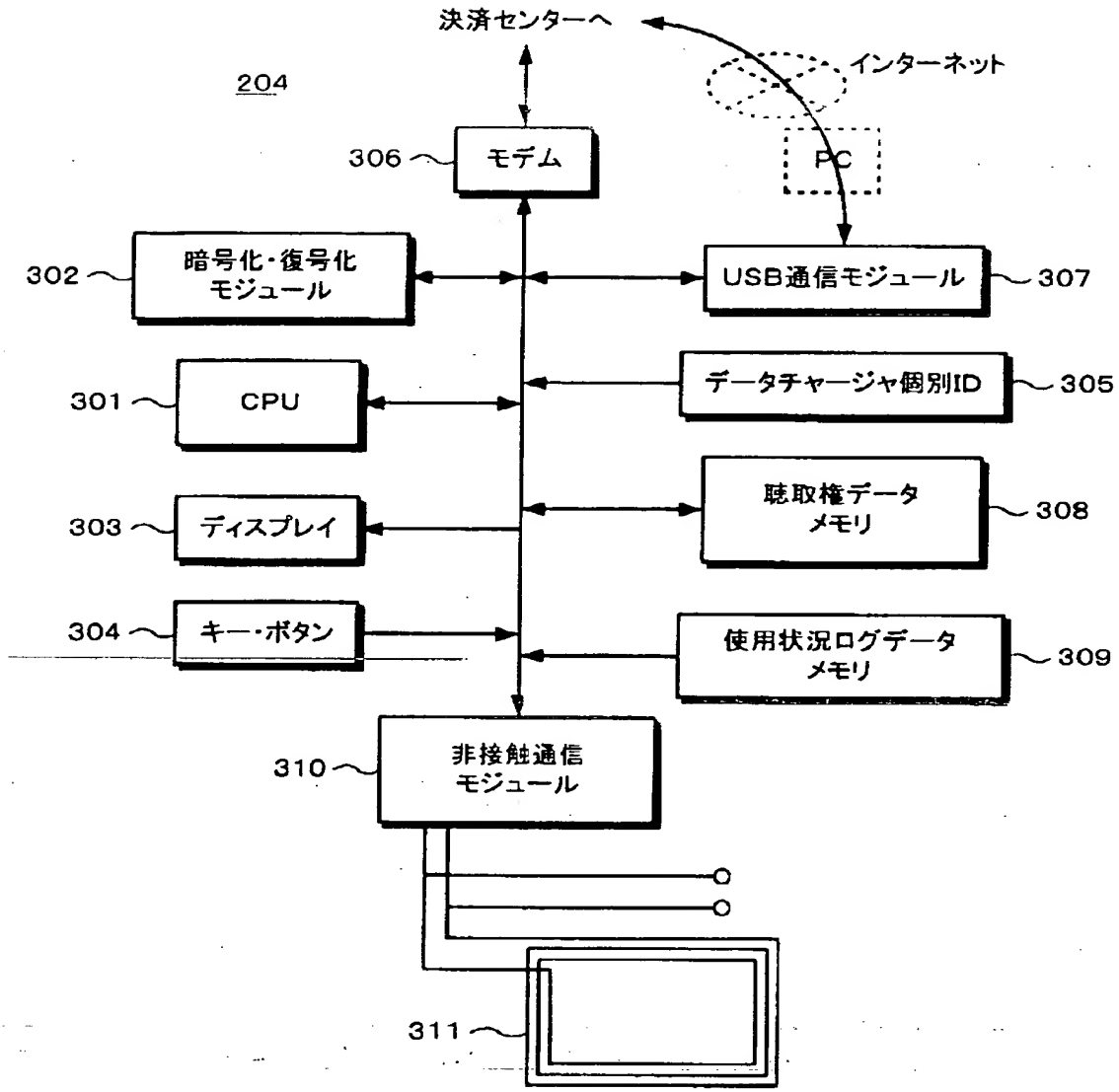
【図６】


コピー出力
アナログオーディオ
18
202:セキュアデコーダ
D／A
13
伸長器
12
復号器
11
通信部
17
制御部
14
メモリ部
16
I／F
15
201
I／F
2
媒体
1
MODEM
25
メモリ部
24
システムコントローラ
21
ディスプレイ
23
操作部
22

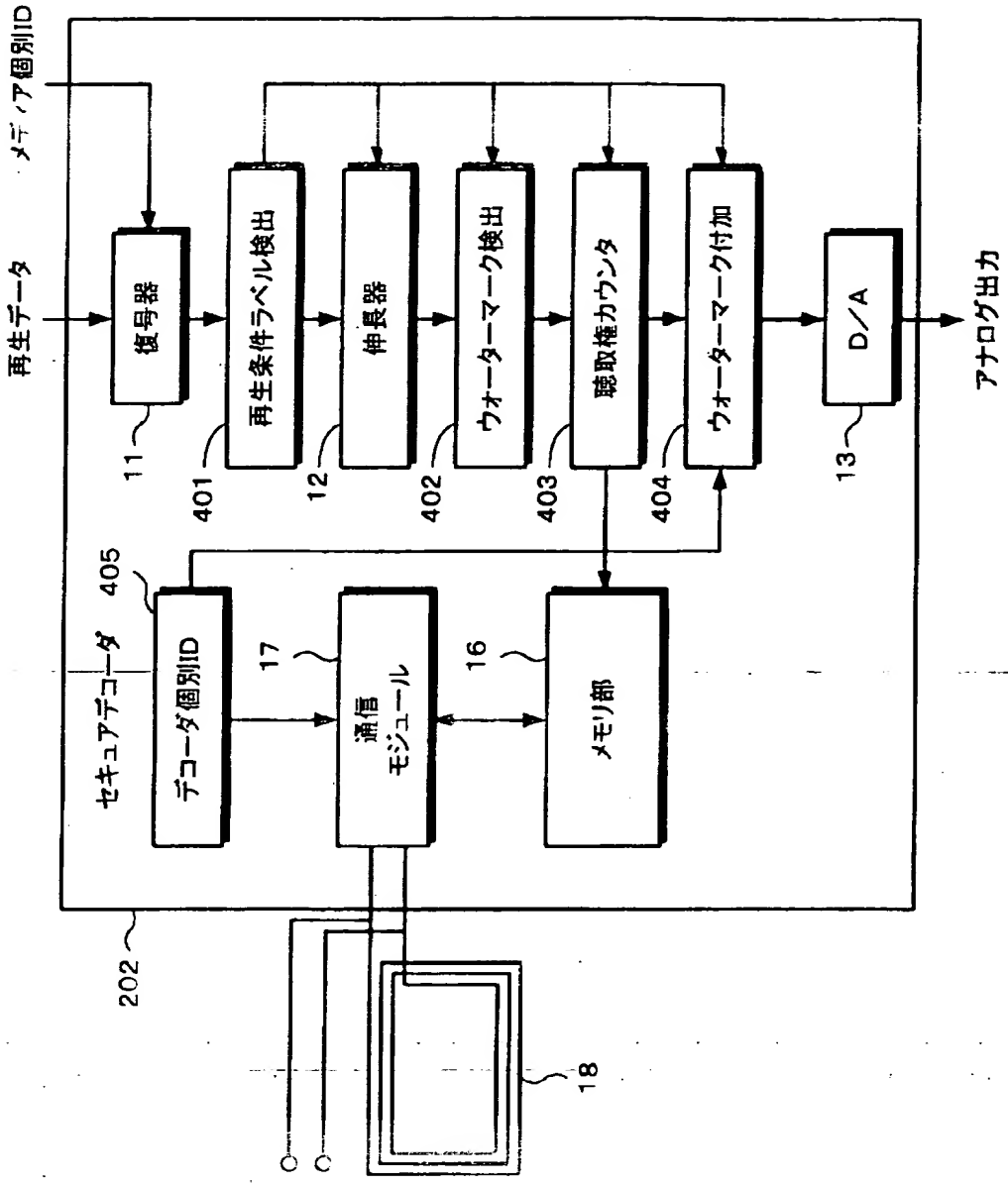
【図７】


再生スタンバイ
S1
再生か？
S2
NO
YES
無料再生用ｺﾋﾟｰか？
S3
NO
YES
課金再生用コピー出力
S5
出力禁止
S4
課金処理OK？
S6
NO
YES
無料再生不可
S7
再生課金条件提示
S8
買取りか？
S9
NO
YES
月極契約有？
S13
NO
YES
月極契約内楽曲か？
S14
NO
YES
買取り用課金
S10
暗号の復号化
S11
暗号の復号化
S15
暗号の復号化
S17
無料再生
無料再生用ｺﾋﾟｰ不可、ﾑｰﾌﾞ可
S12
無料再生
課金再生用コピー可
S16
課金再生
課金再生用コピー可
S18

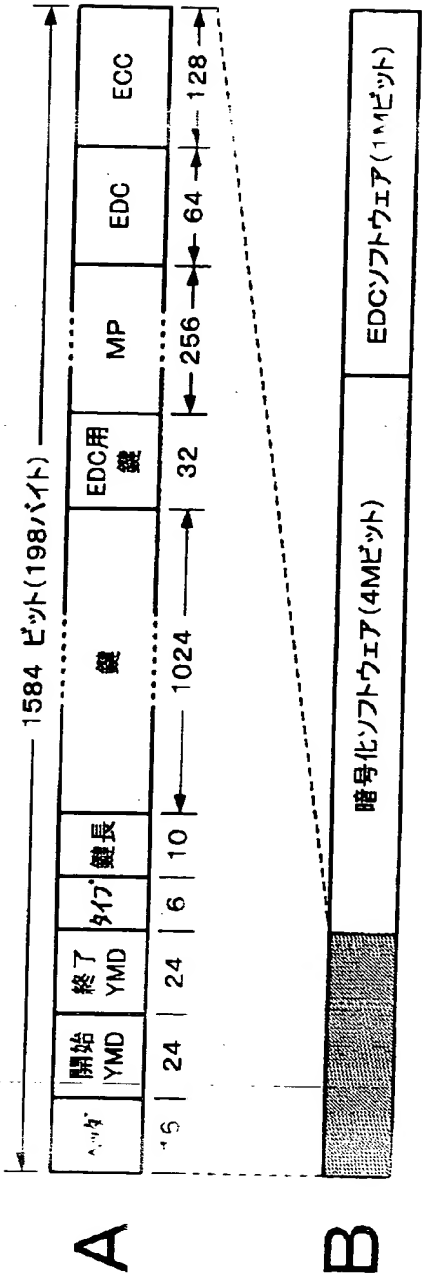
【図８】


決済センターへ
インターネット
204
306
モデム
PC
302
暗号化・復号化
モジュール
USB通信モジュール
307
301
CPU
データチャージャ個別ID
305
303
ディスプレイ
聴取権データ
メモリ
308
304
キー・ボタン
使用状況ログデータ
メモリ
309
310
非接触通信
モジュール
311

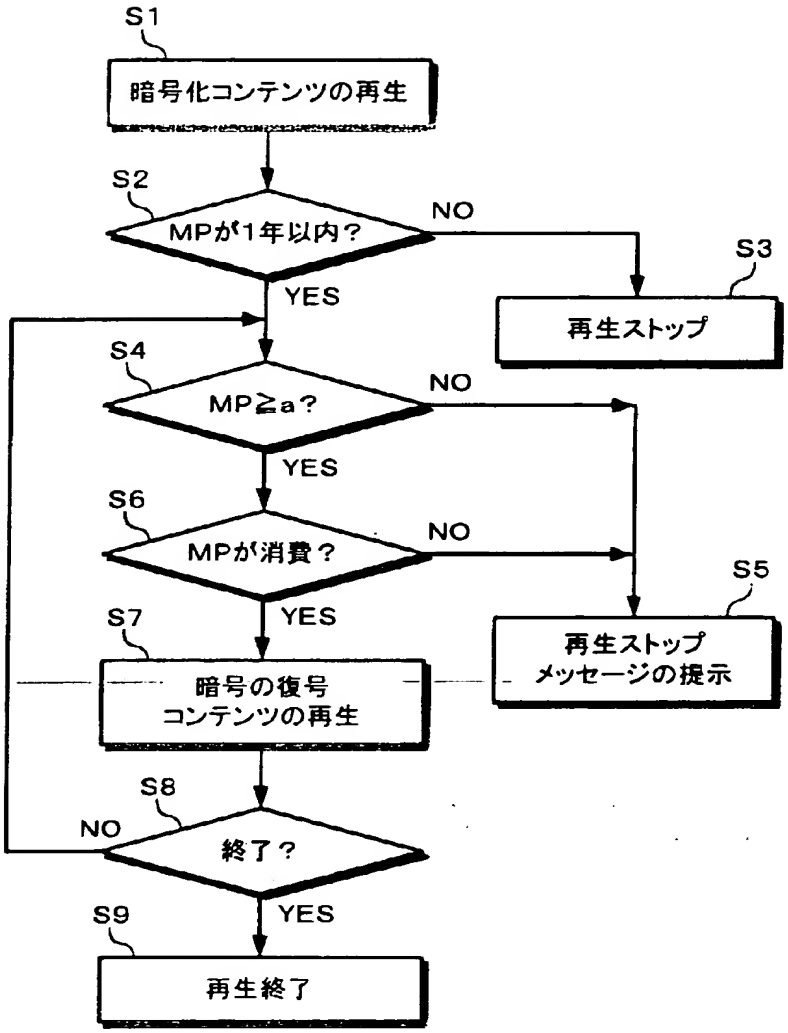
【図９】


メディア個別ID
再生データ
復号器
11
再生条件ラベル検出
401
伸長器
12
ウォーターマーク検出
402
聴取権カウンタ
403
ウォーターマーク付加
404
D／A
13
アナログ出力
405
セキュアデコーダ
デコーダ個別ID
17
通信モジュール
16
メモリ部
202
18

【図１０】


1584 ビット(198バイト)
開始 YMD
24
終了 YMD
24
タイプ
6
鍵長
10
鍵
1024
EDC用 鍵
32
MP
256
EDC
64
ECC
128
A
B
暗号化ソフトウェア(4Mビット)
EDCソフトウェア(1Mビット)

【図１１】


S1
暗号化コンテンツの再生
S2
MPが1年以内？
NO
S3
再生ストップ
YES
S4
MP≧a？
NO
YES
S6
MPが消費？
NO
S5
再生ストップ
メッセージの提示
YES
S7
暗号の復号
コンテンツの再生
S8
NO
終了？
YES
S9
再生終了

【書類名】　要約書

【要約】

【課題】　電子マネー、電子利用権のセキュリティを向上する。

【解決手段】　先頭にヘッダが位置し、次に、聴取権データの有効な期間を規定するために、開始年月日と終了年月日とが順に配置される。続くタイプが暗号化の種類を表す。その後に、鍵長が配され、その後に鍵が配置される。そして、ＥＤＣ用の鍵と、それに続いて２５６ビットの暗号化された聴取権データＭＰが配される。データＭＰの後にＥＤＣとＥＣＣとが順に配置される。また、暗号化を行うためのソフトウェア（４Ｍビット）が配され、さらに、暗号化のソフトウェアに対するＥＤＣソフトウェア（１Ｍビット）が配される構成も可能である。聴取権データのセキュリティ開始ＹＭＤ、鍵長、鍵、ＥＤＣ用鍵の内の少なくとも１つをセンターが定期的、または非定期で変更可能とする。聴取権データのセキュリティを変更した後では、旧いセキュリティの聴取権データが無効となり、旧い聴取権データでは、コンテンツを利用できないようになされる。

【選択図】　図１０

出証特２０００－３０７５４７９

出　願　人　履　歴　情　報

識別番号　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社